

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Petition of the Cellular Telecommunications	)	WT Docket No. 01-72
Industry Association for a Rulemaking to	)	DA-01-696
Establish Fair Location Information Practices	)	
	)	

**COMMENTS OF THE  
CENTER FOR DEMOCRACY AND  
TECHNOLOGY**

James X. Dempsey  
The Center For Democracy & Technology  
1634 Eye Street NW, Suite 1100  
Washington, DC 20006  
(202) 637-9800  
[www.cdt.org](http://www.cdt.org)

Deirdre Mulligan  
Christopher K. Ridder  
Eddan Katz  
Samuelson Law, Technology and Public  
Policy Clinic  
University of California, Berkeley  
School of Law (Boalt Hall)  
392 Simon Hall  
Berkeley, CA 94720  
(510) 848-1501

## **TABLE OF CONTENTS**

I. Introduction	1
II. Wireless Location Information Presents Particularly Sensitive Privacy Concern	2
III. Section 222 Contains Important Privacy Protections That Need To Be Further Explicated	5
IV. Simple, Clear FCC Rules Will Foster the Development of New Information-Based Services By Buttressing Consumer Confidence and Creating a Level Playing Field Among Competitors	7
V. A Separate Rulemaking Is Appropriate Because Wireless Location Information Privacy Is Governed By Different Statutory Language And Involves a Different Set of Industry Players	9
VI. Technology Neutrality Should Be A Feature Of These New Rules	9
VII. Conclusion	10

## **I. SUMMARY AND INTRODUCTION**

The Center for Democracy and Technology (CDT) submits these comments in support of the Cellular Telecommunications Industry Association's petition to commence a separate rulemaking to establish technology neutral privacy regulations for wireless location information. CDT is a non-profit 501(c)(3) organization dedicated to advancing individual liberties and democratic values in new communications media. Since its inception in 1994, CDT has advocated for strong privacy rules that give individuals control over the collection, use and disclosure of personal information.

CDT believes that a separate proceeding to craft strong, technology neutral privacy rules implementing the wireless location information provisions of section 222 of the Communications Act should commence immediately for the following reasons:

- Wireless location information poses uniquely sensitive privacy concerns.
- Section 222 contains important privacy protections that should guide the design and deployment of wireless location based services.
- A consistent and predictable set of privacy rules is necessary to protect consumers and create a level playing field across all devices and platforms. The lack of such a framework undermines consumer privacy and confidence and poses an unacceptable risk of inappropriately skewing the marketplace and the development of new services.
- A rulemaking on wireless privacy separate from other FCC proceeding on CPNI is appropriate because wireless location information privacy is governed by different statutory language and involves a different set of industry players.
- Technology neutrality is critical to ensure that Congress's intent to protect the privacy of location information is realized.

For these reasons, CDT urges the Commission to commence a separate rulemaking for the purpose of creating strong, technology neutral rules to implement the privacy protections for wireless location information in section 222.

## **II. WIRELESS LOCATION INFORMATION PRESENTS PARTICULARLY SENSITIVE PRIVACY CONCERNS**

The development of wireless location based products and services, for all their convenience and usefulness, introduces new and heightened privacy risks for consumers that must be addressed. The portability of mobile devices and the ubiquity of their applications coupled with their ability to pinpoint the location of individuals and reveal it to others could, in the absence of clear privacy rules, produce a system where the everyday activities and movements of individual consumers are tracked and recorded. Wireless location technology has the potential to take data collection to new heights, allowing records to be compiled not just about discrete transactions but about individuals' whereabouts.

It is increasingly apparent that products and services that use location information will soon pervade everyday life. People can begin the day driving to work using traffic and map services in their automobiles, such as GM Onstar, which allow their exact route to be monitored and recorded.<sup>1</sup> Passing through a wireless tollbooth collection system, such as EZ-Pass or FasTrak, the exact moment an individual crosses a bridge or tunnel can be pinpointed and recorded.<sup>2</sup> During the course of the day, the information services available through personal digital assistant (PDA) devices and cellular phones will identify the individual's precise location – perhaps only when specific stores and restaurants are sought using wireless directory services or

---

<sup>1</sup> The GM Onstar (<http://www.onstar.com/>) vehicle navigation system can be used for its mapping capabilities, for safety in emergency situations, and security in case of auto theft. Already companies like Telcontar (<http://www.telcontar.com/>), which makes map engine software, market their product for the potential commercial uses in advertising.

<sup>2</sup> For a listing of electronic toll collection systems in various countries and states, see <http://www.ettm.com/links.html>. Transcore, one of the leading providers of toll collection systems, also markets their products for use in automatic vehicle registration, tracking of vehicles for emission controls, as well as commercial uses such as drive-through payments for things like food, gas, and car washes (<http://www.transcore.com/whoweare/index.htm>)

due solely to their “always on” nature.<sup>3</sup> Instant messaging services will make an individual's location available to friends, but also potentially to advertisers.<sup>4</sup> Bluetooth-enabled devices will support services such as money transfers between individuals and networking.<sup>5</sup> Each Bluetooth-enabled interaction will indirectly reveal the individual's physical location to the device, and corresponding individual or entity, with which it interacts. The location information created by these various interactions can be collected and used by a variety of companies and later accessed by private parties or government agencies without the individual's knowledge or consent.

Location-based services will bring many advantages and the potential for desirable new services and applications, but at the same time poses unique risks. For example, wireless location services present a unique opportunity for advertisers to bridge the prediction of a consumer's preferences and buying patterns with direct marketing targeted to the exact moment and location of the consumer. This relationship between the marketer and the consumer can be mutually beneficial, but its desirability and acceptability depends on the consumer's control over the advertising to which they are exposed. Consumers are already dissatisfied with the volume of unsolicited marketing directed to them by mail, telephone, and email.<sup>6</sup> Consumers' dissatisfaction

---

<sup>3</sup> Index Only Technologies (<http://www.indexonly.com/>), Via-Vis Mobile Solutions (<http://www.viavis.com/>), and ClickADeal.com (<http://www.clickadeal.com/>) are introducing location-based business directory information with specialized services such as nearby gas stations, restaurants, and other stores along their price comparisons and coupons. GeePS (<http://www.geeps.com/>) markets its wireless promotional systems to work within a shopping center. GoAmerica (<http://www.lawonthego.com/>) even provides wireless Lexis access.

<sup>4</sup> Companies such as Invertix (<http://www.invertix.com/>) and iProx (<http://www.iprox.com/>) have developed Instant Messaging software products for mobile phones that alert other subscribers on an individual's buddy list when they are in near proximity.

<sup>5</sup> VoiceFlash Networks, Inc. (<http://www.registrymagic.com/>) market point-of-sale Bluetooth solutions for credit card transfers. Zebypass (<http://www.zebrapass.com/>) provides wireless ticketing and promotion solutions to sports, entertainment, and retail companies.

<sup>6</sup> In a recent survey conducted by AdTech and Talk City, 29 percent said they did not find any form of online marketing intrusive while 71 percent found some advertising to be intrusive. (See [http://www.nua.ie/surveys/index.cgi?f=VS&art\\_id=905355401&rel=true](http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905355401&rel=true))

is likely to be heightened when the advertisements arrive from third parties with whom the consumer has not established any relationship. Without awareness of how their location information is being used and who has access to it, consumers will feel as though there is omnipresent surveillance of their activities by companies they do not know. The invasiveness of such advertising increases when the volume and frequency of messages is also outside of their control. Since location information may simultaneously be collected by a number of companies, such as the wireless carrier and the information service provider, consumers will be confused about who has access to their information. Consumers are likely to find wireless solicitors tracking and targeting particularly invasive.

As distinct from existing forms of CPNI, wireless location information data can be collected everywhere and at any time.<sup>7</sup> While individuals must actively place a telephone call, the seamless integration of wireless services can operate without the need for an individual to actively trigger the disclosure of location information. Rules that require location information service providers to adhere to strong privacy rules are necessary to counterbalance the invisible nature of such data collection.

The availability of location information presents unique risks to individuals. Without the ability to control the collection of location information, consumers may lose the privacy safeguards currently afforded by other federal and state privacy laws. For example, location information reveals physical destinations such as medical clinics or government services

---

<sup>7</sup> Digital Angel (<http://www.digitalangel.net/>) markets products designed to be placed directly on individuals so that they can be constantly tracked.

buildings.<sup>8</sup> These destinations imply additional information about an individual.<sup>9</sup> In some cases the information implied from location information reveals information, such as health condition, that is generally afforded protection by laws that limit access to such data.

Information in databases is subject to a wide range of risks, requiring appropriate privacy and security measures. The risks include misuse by insiders,<sup>10</sup> unintentional or mistaken disclosure,<sup>11</sup> and access by unauthorized individuals.<sup>12</sup> Because location information reveals, often in real-time, the whereabouts of the individual, the potential for privacy intrusion and other harms is more serious than with other types of personal information. In extreme cases, improper disclosure of location information could place a person in physical danger; location information could be misused by stalkers or in domestic violence cases.

### **III. SECTION 222 CONTAINS IMPORTANT PRIVACY PROTECTIONS THAT NEED TO BE FURTHER EXPLICATED**

In the Wireless Communications and Public Safety Act of 1999 (WCPSA), Congress deemed wireless location information CPNI. Moreover, Congress at the same time amended Section 222 to explicitly require "express prior authorization" before a user of a commercial

---

<sup>8</sup> See Simon Romero, *Locating Devices Gain in Popularity but Raise Privacy Concerns*, N.Y. Times, March 4, 2001. Available at <http://www.nytimes.com/2001/03/04/technology/04LOCA.html>.

<sup>9</sup> The privacy risks increase when information is collected over prolonged periods of time. It has been reported that CalTrans has not erased the FasTrak data it has collected since it launched the system four years ago. See Todd Wallack, *They Know Where You've Been: Data Collected From FasTrak Drivers Raise Privacy Concerns*, San Francisco Chronicle, Feb. 12, 2001.

<sup>10</sup> A recent Information Security survey revealed that information theft by insiders in a company poses greater threats than external security breaches. 24% of respondents reported electronic theft or sabotage of proprietary information; 58% reported abuse of employee computer access controls. Information Security, *Security Focused*, Sept. 2000, at p.47. Available at [http://www.infosecuritymag.com/articles/september00/pdfs/Survey1\\_9.00.pdf](http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf).

<sup>11</sup> Kaiser Permanente recently admitted that it mistakenly sent emails containing sensitive information to the wrong people. See Bill Brubaker, *Sensitive Kaiser E-mails Go Astray*, Washington Post, August 10, 2000, at E1.

<sup>12</sup> A private investigator was able to get information about an E-ZPass user in less than an hour. See Danielle Furfaro and Edward Fitzpatrick, *E-Zpass Data Not Hard to Crack*, The Times Union. Nov. 28, 1999.

mobile service will be deemed to have consented to use or disclosure of or access to wireless location information.

The express prior authorization rule in section 222 is, of course, self-executing, and normally a statute like this might not require further FCC action. But it is clear that the rule has not been adequately noticed by some in industry and has generated uncertainty among some of those who are aware of it. This confusion is perhaps part of the broader confusion in the Internet, telecommunications and information industries over the meaning and application of basic privacy principles.

The rules set out in Section 222(c) embody several important principles of fair information practices – the underlying framework of most privacy laws in the United States and abroad.<sup>13</sup> Section 222(c)(1) requires that: individuals be given notice of the collection of information and its intended uses; businesses use information solely for the consumer initiated transaction; businesses gain individual's permission (an "opt-in" standard) prior to using personal information for secondary purposes – such as marketing; and that businesses gain individuals' permission (an "opt-in" standard) prior to disclosing personal information to third parties. Section 222(c)(2) requires businesses to provide consumers access to the information stored about them.

These principles are necessary to ensure that individuals' privacy expectations are met as wireless location services are developed and deployed. They are especially important in the wireless location context, where the information can be used for pervasive tracking of consumers.

---

<sup>13</sup> For detailed information on fair information practices, see, e.g., *Organisation for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (5/00), available at <<http://www.ftc.gov/os/2000/05/index.htm#22>>

Specific rules regarding implementation of fair information practices are needed to ensure predictability and consistency in the marketplace.

#### **IV. SIMPLE, CLEAR FCC RULES WILL FOSTER THE DEVELOPMENT OF NEW INFORMATION-BASED SERVICES BY BUTTRESSING CONSUMER CONFIDENCE AND CREATING A LEVEL PLAYING FIELD AMONG COMPETITORS**

The developing market of location-based services has yet to establish standards and market leaders for the technologies that transmit and collect location information. It is likely that a variety of wireless devices will provide services that are indistinguishable to the consumer. In order to maintain a consistent privacy regime for consumers, wireless location information collection must be regulated across the diversity of spectrum and technologies that will provide those services. Consumer confidence in adopting new technologies will be adversely affected if the general public perceives the new products as immune to the privacy protections of their other wireless devices.<sup>14</sup> Inconsistent privacy regulation of similar services may lead to a general mistrust of wireless devices.

Uniform privacy regulations are also necessary to ensure competition in a nascent market. Location based services that are regulated may be disadvantaged by the increased operational costs of conforming with privacy regulations. When the consumer is faced with a choice between less expensive applications for similar services, the privacy standards for technologies under regulation will be undermined by arbitrary competitive advantages for unregulated devices.<sup>15</sup> The

---

<sup>14</sup> See M.J. Zuckerman, *Wireless, With Strings Attached*, USA Today, Feb. 7, 2001.

<sup>15</sup> A Texas car insurance company offers lower rates for drivers who agree to have their driving habits monitored. See *Big Brother Calling: Location Technology in Devices Such As Cell Phones Will Make You Easy to Find*, Business Week, Sept. 25, 2000, available at [http://www.businessweek.com/2000/00\\_39/b3700104.htm](http://www.businessweek.com/2000/00_39/b3700104.htm).

FCC must create a level-playing field for the various technologies using location information so that the most competitive and innovative products can succeed in the marketplace.

It is clear from Section 222 which standard applies to wireless location information -- "express prior authorization." However, there are currently no regulatory guidelines and no safe-harbors for how the standard should be implemented. If the Commission delays in issuing implementing rules, the wireless location industry could be forced to retrofit its systems when rules are developed. Consumers could later be forced to change their practices and expectations. Service contracts may need to be renegotiated.

By acting now, the Commission will help a rapidly evolving location services industry and its customers. Rules implementing Section 222 would provide a clear framework for industry to design its devices and services, avoiding potential need to retrofit or redesign. And they would help consumers by informing them in a predictable and reliable way how their location information will be handled.

**V. A SEPARATE RULEMAKING IS APPROPRIATE BECAUSE WIRELESS LOCATION INFORMATION PRIVACY IS GOVERNED BY DIFFERENT STATUTORY LANGUAGE AND INVOLVES A DIFFERENT SET OF INDUSTRY PLAYERS.**

CDT urges the Commission to keep the wireless location issue separate from the CPNI docket, for several reasons. First, the new express prior authorization language is different from the "customer approval" standard governing the rest of the Commission's CPNI docket. With regard to wireless location information, it is quite clear that an opt-in standard is required.<sup>16</sup> Second, Section 222 applies specifically to wireless systems, while the rest of the CPNI docket is

focused on a wide range of wireless and cable-based systems. Because of the uniquely wireless nature of Section 222, CDT agrees with CTIA that different entities are likely to comment on these rules than would normally comment on the CPNI docket. Finally, time is of the essence with regard to wireless location information. New systems that cross a wide range of platforms are currently being rolled out across the country. Specific rules will protect privacy and help to ensure that new wireless location services will not have to scramble after the fact to be in compliance.

## **VI. TECHNOLOGY NEUTRALITY SHOULD BE A FEATURE OF THESE NEW RULES**

Technology neutrality is crucial for any rules concerning the privacy of location information. Widespread convergence of devices and communications platforms is, if anything, more accelerated in the wireless field. Cellular telephones, personal digital assistance (PDAs), devices like the Blackberry email pager, in-vehicle devices and other handheld devices can easily be configured with an embedded GPS chip or other technology capable of generating location information.

CDT believes that these technologies promise great benefits to consumers, provided the privacy and safety risks are addressed through regulations implementing Section 222. However, in order to be effective, the rules promulgated by the Commission should encompass the entire range of devices and methods of transmitting location information.

Consumers cannot be expected to distinguish between devices and services that are subject to varying privacy protections based on arbitrary regulatory classifications. Rather, consumers should be confident that, whenever they are using a device that relays location

---

<sup>16</sup> CDT believes that an "opt-in" standard is required for all CPNI data, however the language applied to location

information, its use, disclosure and access will be governed by predictable, easily understandable privacy rules. Technology neutrality is essential given the wide range of devices and means for transmitting location information.

Technology neutrality also ensures a level playing field in the market for location-based services. It would be unfair to subject service providers to different regulatory schemes because of the technology employed. If one provider were subject to regulations while another is not, the unregulated provider could gain an unfair competitive advantage. The market should select the best location-based services free of any disparity imposed by inconsistent regulation.

## **VII. CONCLUSION**

CDT believes that a separate proceeding to craft strong, technology neutral privacy rules implementing section 222 should commence. It is in the interest of both consumers and the wireless location industry to issue clear guidelines implementing the strong privacy protections afforded by section 222 in a technology neutral fashion. Location information presents unique risks to privacy and potential for other forms of harm. Wireless location information is governed by separate statutory language. For these reasons the FCC should act on CTIA's petition and commence a separate rulemaking.

Respectfully submitted,

James X. Dempsey  
The Center For Democracy & Technology  
1634 Eye Street NW, Suite 1100  
Washington, DC 20006  
(202) 637-9800

Deirdre Mulligan  
Christopher K. Ridder  
Eddan Katz  
Samuelson Law, Technology and Public  
Policy Clinic

---

data is even clearer on this point than the language governing CPNI data generally.

[www.cdt.org](http://www.cdt.org)

University of California, Berkeley  
School of Law (Boalt Hall)  
392 Simon Hall  
Berkeley, CA 94720  
(510) 848-1501

April 6, 2001